UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/723,521 | 11/26/2003 | Ron Ben-Natan | GRD03-01 | 8680 |

7590 06/18/2007

Barry W. Chapin, Esq.
CHAPIN & HUANG, L.L.C.
Westborough Office Park
1700 West Park Drive
Westborough, MA 01581

| EXAMINER | |
|---|---|
| KIM, PAUL | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2161 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 06/18/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/723,521 | BEN-NATAN, RON | |
| | Examiner | Art Unit | |
| | Paul Kim | 2161 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *23 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-8,11-30 and 33-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,11-30 and 33-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

SAM RIMELL
PRIMARY EXAMINER

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This Office action is responsive to the following communication: Amendment filed on 23 March 2007.

2. Claims 1-8, 11-30, and 33-46 are pending and present for examination.

### *Continued Examination Under 37 CFR 1.114*

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 23 March 2007 has been entered.

### *Response to Amendment*

4. Claims 1, 20, 24, 40-43 and 46 have been amended.

5. Claims 9-10 and 31-32 have been cancelled.

6. No claims have been added.

### *Claim Rejections - 35 USC § 112*

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. **Claims 1, 20, 24, 40-43** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. As noted in the Examiner Interview conducted on 23 January 2007, the aforementioned claims are replete with condition "if" statements which effectively optionally recite the

occurrences of the related conditions. Accordingly, it is unclear as to scope of the claimed invention, particularly when said "if" statements are not satisfied. Applicant is advised to use more definitive terminology such as "when."

### *Claim Rejections - 35 USC § 101*

9. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. **Claim 1-8, 11-30, and 33-46** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed toward "a method of security enforcement for a persistent data repository," and are non-statutory because they do not encompass tangible subject matter and/or embodiments which fall within a statutory category.

As per claims 1-8, 11-30, and 33-46, the claims fail to recite a "useful, concrete and tangible result" in that the claims fail to recite the return of the limited data access transaction results as limited by the security policy. That is, while specified data may be eliminated from the results, the claims as recited fail to provide a method step wherein a user application receives said results. See State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. MPEP 2106. "The claimed invention as a whole must accomplish a practical application. That is, it must produce a 'useful, concrete and tangible result' " (emphasis added).

As per claims 41-42, the claims are directed toward "[a] computer program product" and "[a] computer readable medium" such that both constitute software, per se. See State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. MPEP 2106. "The claimed invention as a whole must accomplish a practical application. That is, it must produce a 'useful, concrete and tangible result' " (emphasis added). It is noted that the limitations of the claims may be considered to be software, per se, since the claims fail recite a computer readable medium which is integrated into a computer hardware system and

executed. Since a computer program is merely a set of instructions capable of being executed by a program, the computer program itself is not a process and is nonstatutory functional descriptive material.

### *Claim Rejections - 35 USC § 103*

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 1, 5-6, 8, 11-12, 15, 17-19, 24, 28-29, 33-35, 38-39, and 42-46** are rejected under 35 U.S.C. 103(a) as being unpatentable over Fisher et al (U.S. Patent No. 6,085,191, hereinafter referred to as FISHER), filed on 25 March 1998, and issued on 4 July 2000, in view of Hippelainen (USPGPUB No. 2002/0078384, hereinafter referred to as HIPPELAINEN), filed on 10 July 2001, and issued on 20 June 2002.

13. **As per independent claims 1, 24, 33**, FISHER, in combination with HIPPELAINEN, discloses:

A method (and computer program product, computer data signal, or data security filter device) of security enforcement for a persistent data repository comprising:

> intercepting, in a nonintrusive manner {See FISHER, C27:L54-59, wherein this reads over "[n]o information is returned to the user for other objects in the database, and thus the user is not informed that access has been denied to any objects. This is important, because the user must not be informed of even the existence of objects that are not within his purview"}, a data access transaction between a user application and a data repository having data items {See FISHER, C28:L53-64, wherein this reads over "[s]tep 1612 represents the action of the DBMS trigger, which intercepts a user access request to access management information stored in managed objects stored in a desired table in the database"};
>
> determining if the intercepted data access transaction corresponds to a security policy, the security policy indicative of restricted data items in the data repository to which the user application is prohibited access {See FISHER, C28:L37-64, wherein this reads over "[t]he permission objects collectively store information that specifies the access rights by users to specified sets of the managed objects" and "[s]tep 1614 represents the action of the access control procedure 404, which limits access to the management information stored in the set of database tables"}; and
>
> limiting, based on the security policy, the data access transaction by modifying the data access transaction such that data indications, in the data access transaction, corresponding to restricted data items, according to the security policy, are modified in a resulting data access transaction {See FISHER, C28:L65-68, wherein this reads over "[i]n Step 1618 the access control procedure accesses the management information stored in the subset of the requested rows

for which access is permitted by the user"} according to the security policy, limiting the data access transaction further including:

receiving a set of packets, the packets encapsulating the data access transaction according to layered protocols {See FISHER, C28:L2-12, wherein this reads over "the normal query processing by the database access engine is circumvented and replaced by processing performed by (or initiated by) the access control procedure"};

interrogating and modifying the packets in a nondestructive manner with respect to the application layered protocols, the nondestructive manner preserving an expected application layer protocol encapsulation {See FISHER, C28:L2-12, wherein this reads over "[t]he data read from the DBMS tables by the access control procedure 404 is returned to the requesting user or process in the same way that the data would have been returned if the query have been processed by the database access engine"}; and

padding the packets for accommodating elimination of the restricted data items to generate the resulting data access transaction in a manner preserving encapsulation according to expected application based layered protocols {See HIPPELAINEN, [0038], wherein this reads over "the intercepted data packets may always be padded to a maximum length, which further abstruses *sic* the interception activity"}.

As noted in the Examiner Interview dated 10 January 2007, the conditional "if" statement in the aforementioned claim renders most of the claim optional. That is, if the intercepted data access transaction does not correspond to a security policy, then the data access transaction would not be limited since no security policy would apply. Additionally, it is noted that the method step of padding the packets recites an intended use (i.e. "for accommodating elimination of the restricted data items . . . ") which will not be afforded patentable weight for the purposes of this examination.

The combination of the inventions disclosed in FISHER and HIPPELAINEN would disclose a method of intercepting and limiting a data access transaction, wherein the limiting of the data access transaction is completed by padding the transaction. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the inventions suggested by FISHER and HIPPELAINEN. Additionally, it is noted that it would be inherent to the claimed invention that wherein the interception is to go undetected, that the packets of the data access transaction be modified in such a way that the encapsulation is preserved such that the user would further be able to receive and process the results of the modified data access transaction with the application.

One of ordinary skill in the art would have been motivated to do this modification so that the changes in the data access transaction may be undetectable yet still be modified to include the restrictions of the security policy.

14. **As per dependent claims 5 and 28**, FISHER, in combination with HIPPELAINEN, discloses:

The method of claim 1 wherein the data indications are rows of data retrieved from the data repository, and limiting further comprises:

identifying rows having restricted data items {See FISHER, col. 3, lines 29-35, wherein this reads over "[e]ach view defines a subset of rows in the database tables that are accessible when using this view"}, and

eliminating the identified rows from the data access transaction {See FISHER, col. 19, lines 39-49, wherein this reads over "[v]iews can also be used to limit the columns and rows of database tables that are accessible to users"} such that the resulting data access transaction is a modified query response including rows without restricted data items {See COOK, col. 8, lines 45-50, wherein this reads over "access manager will combine this query with the security rule defined above to form the following modified query"}.

15. **As per dependent claims 6 and 29**, FISHER, in combination with HIPPELAINEN, discloses:

The method of claim 5 wherein the data access transaction is a data query response including a row set and limiting further comprises:

comparing each of the rows in the row set to the rules of the security policy {See FISHER, C28:L58-64, wherein this reads over "access control procedure uses the set of access rights stored in the permissions table to determine which, if any, of the rows of data specified by the intercepted query are accessible by the user"}; and

selectively eliminating rows in the row set including the restricted data items, based on the comparing, to generate a modified query response including a filtered row set {See FISHER, C28:L65-68, wherein this reads over "[i]n Step 1618 the access control procedure accesses the management information stored in the subset of the requested rows for which access is permitted by the user"}.

16. **As per dependent claims 8**, FISHER, in combination with HIPPELAINEN, discloses:

The method of claim 1 wherein the nonintrusive manner is undetectable to the user application and undetectable to the data repository {See FISHER, C27:L54-59, wherein this reads over "[n]o information is returned to the user for other objects in the database, and thus the user is not informed that access has been denied to any objects. This is important, because the user must not be informed of even the existence of objects that are not within his purview"}.

17. **As per dependent claims 11 and 34**, FISHER, in combination with HIPPELAINEN, discloses:

The method of claim 10 wherein generating the resulting data access transaction preserves the encapsulating layered protocol associating the packets without employing a proxy for regenerating the sequence of packets {See FISHER, C12:L63-C13:L2}}.

18. **As per dependent claims 12 and 35**, FISHER, in combination with HIPPELAINEN, discloses:

The method of claim 4 wherein intercepting the data access statement includes

receiving an SQL query {See FISHER, C20:L16-26} and

limiting includes appending conditional selection statements to the SQL query, the conditional selection statements computed from the security policy, to generate the resulting data access transaction {See FISHER, C20:L16-26}

19. **As per dependent claim 15**, FISHER, in combination with HIPPELAINEN, discloses:

The method of claim 1 wherein the nonintrusive manner is such that the intercepting and limiting occurs undetectable to both the source and the destination of the data access transaction {See FISHER, C27:L54-59, wherein this reads over "[n]o information is returned to the user for other objects in the database, and thus the user is not informed that access has been denied to any objects. This is important, because the user must not be informed of even the existence of objects that are not within his purview"}.

20. **As per dependent claims 17, 38**, FISHER, in combination with HIPPELAINEN, discloses:

The method of claim 1 wherein intercepting occurs in a data path between a source of the data access transaction and a destination of the resulting data access transaction, and limiting occurs in a component separate from the source and destination {See FISHER, Figure 10}.

21. **As per dependent claims 18, 39**, FISHER, in combination with HIPPELAINEN, discloses:

The method of claim 17 wherein the component separate from the source and destination is a separate network device than the components corresponding to the source and destination {See FISHER, Figure 10}.

22. **As per dependent claim 19,** FISHER, in combination with HIPPELAINEN, discloses:

The method of claim 1 wherein the restricted data items are eliminated from the resulting data access transaction {See FISHER, C19:L50-56}.

23. **As per dependent claim 28**, FISHER, in combination with HIPPELAINEN, discloses:

The method of claim 1 wherein the data indications are rows of data retrieved from the data repository, and limiting further comprises:

identifying rows having restricted data items {See FISHER, col. 3, lines 29-35, wherein this reads over "[e]ach view defines a subset of rows in the database tables that are accessible when using this view"}, and

eliminating the identified rows from the data access transaction {See FISHER, col. 19, lines 39-49, wherein this reads over "[v]iews can also be used to limit the columns and rows of database tables that are accessible to users"} such that the resulting data access transaction is a modified query response including rows without restricted data items {See FISHER, C28:L65-68, wherein

this reads over "[i]n Step 1618 the access control procedure accesses the management information stored in the subset of the requested rows for which access is permitted by the user"}.

24. **As per dependent claim 29**, FISHER, in combination with HIPPELAINEN, discloses:

The method of claim 5 wherein the data access transaction is a data query response including a row set and limiting further comprises:

comparing each of the rows in the row set to the rules of the security policy {See COOK, col. 8, lines 57-59, wherein this reads over "data manager will format this query as an SQL query and submit it to the database which will return the sales data from rows 1 and 3 of Table 2"}; and

selectively eliminating rows in the row set including the restricted data items, based on the comparing, to generate a modified query response including a filtered row set {See FISHER, C28:L65-68, wherein this reads over "[i]n Step 1618 the access control procedure accesses the management information stored in the subset of the requested rows for which access is permitted by the user"}.

25. **As per dependent claim 42,** see the rejections of related claims 1 and 44 herein.

26. **As per dependent claim 43**, see the related rejections of claims 1, 5 and 45 herein.

27. **As per dependent claim 44,** FISHER, in combination with HIPPELAINEN, discloses:

The method of claim 1 wherein the nonintrusive manner is undetectable to the user application and undetectable to the data repository, the nonintrusive manner such that the intercepting and limiting occurs undetectable to both the source and the destination of the data access transaction, wherein intercepting occurs in a data path between a source of the data access transaction and a destination of the resulting data access transaction, and limiting occurs in a component separate from the source and destination, and the component separate from the source and destination is a separate network device than the components corresponding to the source and destination {See {See FISHER, Figure 10}.

28. **As per dependent claim 45,** FISHER, in combination with HIPPELAINEN, discloses:

The method of claim 1 wherein padding the packet further comprises nondestructively modifying the packet such that the packet appears undisturbed to the receiver {See HIPPELAINEN, [0038], wherein this reads over "the intercepted data packets may always be padded to a maximum length, which further abstruses *sic* the interception activity"}.

29. **As per dependent claim 46,** it would be inherent that a SQL query is modified, the payload of the packet is modified as well. Additionally, it is inherent to the claimed invention that during the modification process that the control information has yet to have been accessed and disturbed. That is, during the process of packets, there is an inherent lag which would provide for a time when the control information is left undisturbed.

30. **Claims 2-4, 7, 14, 16, 25-27, 30, and 37** are rejected under 35 U.S.C. 103(a) as being unpatentable over FISHER, in view of HIPPELAINEN, in further view of Cook et al (U.S. Patent No. 6,820,082, hereinafter referred to as COOK), filed on 3 April 2000, and issued on 16 November 2004,

31. **As per dependent claims 2 and 25**, FISHER, in combination with HIPPELAINEN and COOK, discloses:

> The method of claim 1 wherein the security policy has rules {See COOK, col. 9, lines 2-3, wherein this reads over "[s]ecurity policies can be changed by simply modifying the rules within the rule engine"}, each of the rules including an object, a selection criteria and an action, the action indicative of restricted data items {See COOK, col. 2, lines 61-65, wherein this reads over "a plurality of security rules . . . to determine if the user has authority to perform requested action with respect to the data"}.

32. **As per dependent claims 3 and 26**, FISHER, in combination with HIPPELAINEN and COOK, discloses:

> The method of claim 1 wherein the data indications are references to data items in the data repository {See COOK, col. 5, lines 58-61, wherein this reads over "data obtained from the database to control access to the data by the user"} and limiting further includes qualifying the references to generate a modified request indicative of unrestricted data items, such that successive retrieval operations employing the qualified references do not retrieve restricted data items {See COOK, col. 7, lines 61-64, wherein this reads over "security constraints may be applied to the incoming query and processed in the access manager to form a modified query which is sent to the data manager"}.

33. **As per dependent claims 4 and 27**, FISHER, in combination with HIPPELAINEN and COOK, discloses:

> The method of claim 3 wherein the data access transaction is a data access statement operative to request data and limiting further comprises:
>
> identifying at least one rule, according to the security policy, corresponding to the data access statement, the identified rule restricting access to at least one of the data items indicated by the data access statement {See COOK, Table 1; col. 7, lines 42, wherein this reads over "object-level security applies to an entire row of data"; and col. 8, lines 34-35, wherein this reads over "[t]he rule engine includes the following user defined security rule for Table 2"}, and
>
> concatenating selection qualifiers to the data access statement corresponding to the identified rule, {See COOK, col. 8, lines 45-53, wherein this reads over "access manager will combine this query with the security rule defined above to form the following modified query for a user"} the selection qualifiers operable to omit the restricted data items from the qualified references of the data access statement {See COOK, col. 8, lines 57-59, wherein this reads over "the database which will return the sales data from rows 1 and 3 of Table 2"}.

34. **As per dependent claims 7 and 30**, FISHER, in combination with HIPPELAINEN and COOK, discloses:

> The method of claim 2 wherein the actions are selectively indicative of modifications, the modifications further comprising attributes, operators, and operands, the limiting further comprising
>
> > identifying data items corresponding to the attributes, each of the attributes associated with an operator and an operand {See COOK, col. 8, lines 51-53};
> >
> > applying an operator specified for the data item to the operand specified for the data item {See COOK, col. 8, lines 51-53}; and
> >
> > determining, as a result of applying the operator, whether to eliminate the identified data item {See COOK, col. 8, lines 51-53}.

35. **As per dependent claims 14 and 37**, FISHER, in combination with HIPPELAINEN and COOK, discloses:

> The method of claim 6 wherein intercepting the data query response further comprises:
>
> > intercepting the data query response from the data repository as the data access transaction {See FISHER, col. 28, lines 53-64, wherein this reads over "Step 1612 . . . which intercepts a user access request to access management information stored in managed objects stored in a desired table in the database"},
> >
> > the data query response encapsulated as a row set having rows from a relational database query {See COOK, col. 8, lines 57-59, wherein this reads over "return the sales data from rows 1 and 3"} and further wherein limiting includes
> >
> > > discarding rows in the row set having restricted data items {See COOK, col. 8, lines 45-50, wherein this reads over "access manager will combine this query with the security rule defined above to form the following modified query"} and
> > >
> > > transmitting the remaining rows to the user as the resulting data access transaction {See COOK, Figure 6, step 122; and col. 11, lines 10-12, wherein this reads over "[t]he page generator outputs a page formatted using visible data from the database"}.

The combination of the inventions disclosed in FISHER, HIPPELAINEN, and COOK would disclose a method wherein the data query response from the data repository is intercepted and rows are discarded accordingly. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the inventions suggested by FISHER, HIPPELAINEN, and COOK.

One of ordinary skill in the art would have been motivated to do this modification in so that restricted data items may be eliminated and the remaining rows transmitted to the user.

36. **As per dependent claim 16**, FISHER, in combination with HIPPELAINEN and COOK, discloses:

The method of claim 1 wherein intercepting further comprises:

establishing an identification exchange intended for interception and operable to transmit an identification token indicative of an application user {See COOK, Tables 3 and 4; col. 4, lines 60-61, wherein this reads over "the user . . . is identifiable by a user ID"; and col. 8, lines 34-53}; and

parsing, as part of the intercepting, the identification exchange to extract the identification token {See COOK, Tables 3 and 4, and col. 8, lines 34-53}, wherein the identification exchange is benign to the data repository {See COOK, col. 10, line 66 – col. 11, line 13, wherein this reads over "further filter the data returned from the database by removing information that is not available to the user"}.

37. **Claim 13** is rejected under 35 U.S.C. 103(a) as being unpatentable over FISHER, in view of HIPPELAINEN, and in further view of Slutz (U.S. Patent No. 6,581,052, hereinafter referred to as SLUTZ), filed on 2 October 2000, and issued on 17 June 2003.

38. **As per dependent claim 13**, FISHER, in combination with HIPPELAINEN and SLUTZ, discloses:

The method of claim 12 further comprising:

building a parse tree corresponding to the SQL query {See SLUTZ, Figures 6 and 8};

adding nodes in the parse tree corresponding to the appended conditional selection statements {See SLUTZ, col. 11, lines 3-14, wherein this reads over "updates the statement according to the choices made . . . [wherein] a choice at each current node adds a term to the statement's parse tree"}; and

reprocessing the parse tree to generate the resulting data access transaction {See SLUTZ, Figure 6; and col. 9, lines 26-29, wherein this reads over "outputs a representation of the statement to program as the statement is generated"}.

The combination of the inventions disclosed in FISHER, HIPPELAINEN and SLUTZ would disclose a method for building a parse tree corresponding to the SQL query and adding nodes corresponding to the appended conditional selection statements. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the inventions suggested by FISHER, HIPPELAINEN and SLUTZ.

One of ordinary skill in the art would have been motivated to do this modification so that the appended conditional selection statements may be added as nodes to the parse tree.

39. **Claims 20-23, 36 and 40-41** are rejected under 35 U.S.C. 103(a) as being unpatentable over FISHER, in view of SLUTZ.

FISHER differs from the claimed invention in that COOK fails to disclose a method for building a parse tree (claims 20, 36 and 40).

40. **As per independent claims 20 and 40-41**, FISHER, in combination with SLUTZ, discloses:

A method for nonintrusive implementation of data level security enforcement comprising:

defining a security policy between an application and a data repository the security policy having rules indicative of restricted data items, the rules associated with attributes and conditions {See FISHER, C9:L31-39, wherein this reads over "access security rules"};

identifying an entry point between the data repository and the application {FISHER, Figure 10};

deploying a security filter at the entry point, the security filter operable to receive data manipulation messages between the application and the data repository {See FISHER, Figure 10};

the security filter further operable to limit data exposure by the data repository by selectively modifying the data manipulation messages into conformance with the security policy {See FISHER, C28:L2-12, wherein this reads over "[t]he data read from the DBMS tables by the access control procedure 404 is returned to the requesting user or process in the same way that the data would have been returned if the query have been processed by the database access engine"}, the limiting further comprising:

sniffing the entry point to determine data manipulation messages {See FISHER, C28:L2-12, wherein this reads over "the normal query processing by the database access engine is circumvented and replaced by processing performed by (or initiated by) the access control procedure"};

intercepting the sniffed data manipulation messages in a nondestructive manner {See FISHER, C27:L54-59, wherein this reads over "[n]o information is returned to the user for other objects in the database, and thus the user is not informed that access has been denied to any objects. This is important, because the user must not be informed of even the existence of objects that are not within his purview"};

comparing the sniffed messages to the rules in the security policy to determine if the sniffed data manipulation message includes restricted data items {See FISHER, C28:L37-64, wherein this reads over "[t]he permission objects collectively store information that specifies the access rights by users to specified sets of the managed objects" and

"[s]tep 1614 represents the action of the access control procedure 404, which limits access to the management information stored in the set of database tables"};

determining if the sniffed messages match at least one of the rules of the security policy {See FISHER, C28:L37-64, wherein this reads over "[t]he permission objects collectively store information that specifies the access rights by users to specified sets of the managed objects" and "[s]tep 1614 represents the action of the access control procedure 404, which limits access to the management information stored in the set of database tables"};

selectively modifying, if the determining indicates a match between the rules and the data manipulating message, the data manipulation message to remove the matching restricted data item {See FISHER, C19:L0-56}, modifying further including:

building a parse tree corresponding to the SQL query {See SLUTZ, Figures 6 and 8};

adding nodes in the parse tree corresponding to the appended conditional selection statements {See SLUTZ, col. 11, lines 3-14, wherein this reads over "updates the statement according to the choices made . . . [wherein] a choice at each current node adds a term to the statement's parse tree"}; and

reprocessing the parse tree to generate the resulting data access transaction {See SLUTZ, Figure 6; and col. 9, lines 26-29, wherein this reads over "outputs a representation of the statement to program as the statement is generated"}.

The combination of the inventions disclosed in FISHER and SLUTZ would disclose a method for building a parse tree corresponding to the SQL query and adding nodes corresponding to the appended conditional selection statements. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the inventions suggested by FISHER and SLUTZ.

One of ordinary skill in the art would have been motivated to do this modification so that the appended conditional selection statements may be added as nodes to the parse tree.

41. **Claims 21-22** are rejected under 35 U.S.C. 103(a) as being unpatentable over FISHER, in view of SLUTZ, and in further view of COOK.

42. **As per dependent claim 21**, FISHER, in combination with SLUTZ and COOK, discloses:

The method of claim 2 wherein the actions are selectively indicative of modifications, the modifications further comprising attributes, operators, and operands, the limiting further comprising

identifying data items corresponding to the attributes, each of the attributes associated with an operator and an operand {See COOK, col. 8, lines 51-53};

applying an operator specified for the data item to the operand specified for the data item {See COOK, col. 8, lines 51-53}; and

determining, as a result of applying the operator, whether to eliminate the identified data item {See COOK, col. 8, lines 51-53}.

43. **As per dependent claim 22**, FISHER, in combination with SLUTZ and COOK, discloses:

The method of claim 20 wherein modifying further comprises:

reconstructing a request query corresponding to a query syntax {See COOK, col. 8, lines 45-53, wherein this reads over "access manager will combine this query with the security rule defined above to form the following modified query for a user"}; and

adding limiters to the request query corresponding to the matching rules of the security policy {See FISHER, C21:L12-36}, the adding performed in a nondestructive manner such that the modification is undetectable to the data repository {See FISHER, C27:L54-59, wherein this reads over "[n]o information is returned to the user for other objects in the database, and thus the user is not informed that access has been denied to any objects. This is important, because the user must not be informed of even the existence of objects that are not within his purview"}.

44. **Claims 23 and 36** are rejected under 35 U.S.C. 103(a) as being unpatentable over FISHER, in view of SLUTZ, and in further view of HIPPELAINEN.

45. **As per dependent claim 23**, FISHER, in combination with SLUTZ and HIPPELAINEN, discloses:

The method of claim 20 wherein modifying further comprises:

identifying a data retrieval response encapsulated in a layered protocol on the data manipulation message {See FISHER, C28:L2-12, wherein this reads over "the normal query processing by the database access engine is circumvented and replaced by processing performed by (or initiated by) the access control procedure"}; and

reconstructing the data retrieval response by deleting restricted data items from the data retrieval response, the reconstructing performed in a nondestructive manner undetectable to the application and conforming to the encapsulating layered protocol {See HIPPELAINEN, [0038], wherein this reads over "the intercepted data packets may always be padded to a maximum length, which further abstruses *sic* the interception activity"}.

46. **As per dependent claim 36**, FISHER, in combination with HIPPELAINEN and SLUTZ, discloses:

The method of claim 12 further comprising:

building a parse tree corresponding to the SQL query {See SLUTZ, Figures 6 and 8};

adding nodes in the parse tree corresponding to the appended conditional selection statements {See SLUTZ, col. 11, lines 3-14, wherein this reads over "updates the statement according to the choices made . . . [wherein] a choice at each current node adds a term to the statement's parse tree"}; and

reprocessing the parse tree to generate the resulting data access transaction {See SLUTZ, Figure 6; and col. 9, lines 26-29, wherein this reads over "outputs a representation of the statement to program as the statement is generated"}.

The combination of the inventions disclosed in FISHER, HIPPELAINEN, and SLUTZ would disclose a method for building a parse tree corresponding to the SQL query and adding nodes corresponding to the appended conditional selection statements. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the inventions suggested by FISHER, HIPPELAINEN, and SLUTZ.

One of ordinary skill in the art would have been motivated to do this modification so that the appended conditional selection statements may be added as nodes to the parse tree.

***Response to Arguments***

47. Applicant's arguments with respect to claim rejections have been considered but are moot in view of the new ground(s) of rejection.

***Conclusion***

48. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul Kim whose telephone number is (571) 272-2737. The examiner can normally be reached on M-F, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Apu Mofiz can be reached on (571) 272-4080. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Paul Kim
Patent Examiner, Art Unit 2161
TECH Center 2100

SAM RIMELL
PRIMARY EXAMINER